

The Cloud Providers' Challenge

Safeguarding your cloud infrastructure from unmonitored access, malware and intruder attacks grows more challenging as your operation evolves. As your network grows so too does the presence of unsecured privileged identities – those so-called super-user accounts that hold elevated permission to access sensitive data, run programs, and change configuration settings on virtually every component of IT.

Privileged identities exist on all physical and virtual operating systems, on network devices such as routers, switches, and firewalls, and in programs and services including databases, line-of-business applications, Web services, middleware, VM hypervisors, and more.

Left unsecured, privileged accounts leave your organization vulnerable to:

- ▶ IT staff members who have unmonitored access to sensitive customer data and can change configuration settings on critical components of your infrastructure through anonymous, unaudited access.
- ▶ Malware and intruder attacks that can spread rapidly through your infrastructure by exploiting reused and infrequently changed privileged account passwords.
- ▶ Financial loss from failed regulatory audits including PCI-DSS, HIPAA, SOX and other standards that require privileged identity controls.
- ▶ Disruptions in critical IT services whenever manual controls fail to update interdependent accounts or slow the response of your IT staff when they need to access systems for emergency repair.



Privileged Identities Exist on Almost Every Physical and Virtual IT Asset in your Cloud Infrastructure



Control Privileged Identities in the Cloud

Today's Identity Access Management solutions can't manage or secure privileged accounts, but you can quickly take control with **Enterprise Random Password Manager (ERPM™)**. ERPM enables you to continuously discover, update, store, and securely recover every local, domain, and process account password in your cloud infrastructure. With ERPM you can detect each location that privileged account credentials are in use – including physical and virtual computer and network appliance operating systems, applications, databases, web services, tasks, and more – securing each credential and propagating the changes wherever needed, to all interdependent accounts.

No other solution matches ERPM for scalability, breadth of discovery and secure remediation of privileged account passwords. ERPM deploys on your choice of Microsoft and Oracle databases for scalable, transparent operation. It directly authenticates with all major directories to instantly maintain the right levels of access as personnel roles change. And, it offers a reliable three-tier architecture that protects systems across slow WAN links and within network DMZs. New features developed in partnership with cloud service providers include *dual-control multiple tenancy* for fine-grained control over access and reporting by service provider staff and end-customers alike.